

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет математики и компьютерных наук



УТВЕРЖДАЮ:

Проректор по учебной работе,
качеству образования – первый
проректор

подпись

Т.А. Хагуров

«30» мая 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.15 КОМПЬЮТЕРНАЯ АЛГЕБРА И КРИПТОГРАФИЯ

Направление подготовки 02.03.01 Математика и компьютерные науки

Направленность (профиль) Современная алгебра и криптография

Форма обучения очная

Квалификация бакалавр

Краснодар 2025

Рабочая программа дисциплины «КОМПЬЮТЕРНАЯ АЛГЕБРА И КРИПТОГРАФИЯ» составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 02.03.01 Математика и компьютерные науки.

Программу составил(и):
В.А. Любин ст.преподаватель



Рабочая программа дисциплины «Арифметические свойства колец» утверждена на заседании кафедры функционального анализа и алгебры
протокол № 11 «13» мая 2025 г.

Заведующий кафедрой (разработчика) Барсукова В.Ю.



Утверждена на заседании учебно-методической комиссии факультета математики и компьютерных наук
протокол № 4 « 14 » мая 2025г.
Председатель УМК факультета Шмалько С.П.



Рецензенты:

Аршинов Г.А., доктор физ.-мат. наук, профессор кафедры компьютерных технологий и систем КубГАУ –

Марковский А.Н., кандидат физ.-мат. наук, доцент кафедры математических и компьютерных методов КубГУ

1 Цели и задачи изучения дисциплины.

1.1 Цель освоения дисциплины.

Цель освоения дисциплины «Компьютерная алгебра и криптография» – получение базовых теоретических сведений по теории распределения простых чисел, разложения на простые множители, криптосистемы открытого ключа и реализации алгоритмов на подходящих языках программирования.

При освоении дисциплины вырабатывается общематематическая культура: умение логически мыслить, проводить доказательства основных утверждений, устанавливать логические связи между понятиями, применять полученные знания для решения задач криптографии. Получаемые знания лежат в основе математического образования и необходимы для понимания и освоения всех курсов математики, а также для продолжения обучения в магистратуре по соответствующему направлению подготовки.

1.2 Задачи дисциплины.

Дальнейшее формирование у студентов приобретенных на первых двух курсах знаний по фундаментальной, компьютерной алгебре и криптографии.

1.3 Место дисциплины в структуре образовательной программы.

Изучение дисциплины «Компьютерная алгебра и криптография» предусмотрено стандартом высшего профессионального образования специальности 020301 (федеральный компонент в цикле математических и естественных дисциплин). В рамках дисциплины ее изучение базируется на знаниях курса «Фундаментальная и компьютерная алгебра».

1.4 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы.

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине
ПК-1 Способен демонстрировать базовые знания математических и естественных наук, основ программирования и информационных технологий	
ИПК-1.1. Способен решать актуальные и важные задачи фундаментальной и прикладной математики	Знает арифметику целых чисел: делимость, разложение на множители, основную теорему арифметики; структуру кольца многочленов: неприводимость, разложение на множители
	Умеет формировать понятия, взятые из кольца целых чисел и кольца многочленов, для создания криптосистем открытого ключа.
	Владеет способностью определения общих закономерностей разложения элементов кольца на неприводимые множители, владеть структурным анализом в теории колец вычетов и конечных полей.
ПК-5 Способен математически корректно ставить естественнонаучные задачи, знание постановок классических задач математически	

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине
ИПК-5.1. Уметь применять , полученные теоретические знания по арифметике колец вычетов и конечных полей и их взаимосвязи с криптосистемами открытого ключа.	Знает определение основных понятий в данном курсе, формулировки основных теорем с примерами
	Умеет решать задачи по основным разделам курса : генерирование больших простых чисел, разложение на простые множители, создание криптосистем открытого ключа.
	Владеет необходимыми знаниями в программировании для реализации алгоритмов криптосистем открытого ключа.

2. Структура и содержание дисциплины.

2.1 Распределение трудоёмкости дисциплины по видам работ.

Общая трудоёмкость дисциплины составляет 4 зач.ед. (82 час), их распределение по видам работ представлено в таблице

Вид учебной работы		Всего часов	Семестры	
			4	
Аудиторные занятия (всего)		82	82	
В том числе:				
Занятия лекционного типа		18	18	
Лабораторные занятия		34	34	
Иная контактная работа:				
Контроль самостоятельной работы (КСР)		6	6	
Промежуточная аттестация (ИКР)		0,3	0,3	
Самостоятельная работа, в том числе:		23,7	23,7	
Проработка учебного (теоретического) материала		9,7	9,7	
Выполнение домашних заданий (подготовка сообщений, презентаций)		8	8	
Подготовка к текущему контролю		6	6	
Контроль:				
Подготовка к зачету				
Общая трудоемкость	час.	82	82	
	в том числе контактная работа	58,3	58,3	
	зач. ед	4	4	

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины, изучаемые в 6 семестре (очная форма)

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1.	Простые числа, их распределение, генерирование простых чисел.	8	2		4	2
2.	Алгоритмы разложения на простые множители.	9	2		4	3
3.	Дискретный логарифм.	9	2		4	3
4.	Криптосистема RSA и ее реализация.	9	2		4	3
5.	Криптосистема Рабина и ее реализация.	9	2		4	3
6.	El Gamel схема кодирования и ее реализация.	8,7	2		4	2,7
7.	Эллиптические кривые и групповая структура на них.	9	2		4	3
8.	Эллиптические кривые над конечными полями и схема кодирования с помощью эллиптических кривых.	14	4		6	4
	Итого по дисциплине:	75,7	18		34	23,7

2.3 Содержание разделов дисциплины:

2.3.1 Занятия лекционного типа.

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1.	Простые числа, их распределение, генерирование простых чисел.	Теорема распределения простых чисел(PNT) и гипотеза Римана. Тест Ферма и псевдопростые. Числа Карлмайкла. Вероятностный тест на простоту и его реализация. Миллер- Рабин тест на простоту и его реализация.	ПК
2.	Алгоритмы разложения на простые множители.	Поллард ро- метод. Метод Ферма факторизации и его сложность. Квадратичное решето.	ПК
3.	Дискретный логарифм.	Baby-Step Gigant Step алгоритм и его реализация.Поллард ро-метод для дискретного логарифма. Метод индексов для дискретного логарифма и его реализация.	ПК
4.	Криптосистема RSA и ее реализация.	Система кодирования RSA. Генерирование публичных ключей и его реализация. Алгоритм криптосистемы RSA и его корректность. Протокол RSA. Создание криптосистемы RSA.	ПК
5.	Криптосистема Рабина и ее реализация.	Структура квадратов в кольцах вычетов. Квадратичные вычеты. Вычисление квадратных корней в классах вычетов. Алгоритм криптосистемы Рабина. Протокол криптосистемы Рабина. Создание	ПК

		криптосистемы Рабина.	
6.	El Gamel схема кодирования и ее реализация.	Первообразные корни в кольцах вычетов. Вычисления первообразных корней. Алгоритм вычисления первообразных корней и его реализация. Алгоритм кодирования El Gamel. Протокол El Gamel. Создание криптосистемы El Gamel.	ПК
7.	Эллиптические кривые и групповая структура на них.	Групповая структура на эллиптических кривых. Алгоритм сложения точек на эллиптической кривой.	ПК
8.	Эллиптические кривые над конечными полями и схема кодирования с помощью эллиптических кривых.	Построение точек эллиптической кривой над конечным полем. Неравенство Хассе. Дискретный логарифм на эллиптической кривой. Создание криптосистемы на основе эллиптической кривой.	ПК

2.3.2 Занятия семинарского типа. Не предусмотрены

2.3.3 Лабораторные занятия.

№	Наименование раздела	Тематика практических занятий (семинаров)	Форма текущего контроля
1	2	3	4
1.	Простые числа, их распределение, генерирование простых чисел.	Тест Ферма и псевдопростые. Числа Карлмайкла. Вероятностный тест на простоту и его реализация. Миллер-Рабин тест на простоту и его реализация.	РЗ
2.	Алгоритмы разложения на простые множители.	Поллард ро-метод. Метод Ферма факторизации и его сложность. Квадратичное решето. Их реализация.	РЗ
3.	Дискретный логарифм	Baby-Step Gigant Step алгоритм и его реализация. Поллард ро-метод для дискретного логарифма. Метод индексов для дискретного логарифма и его реализация.	РЗ
4.	Криптосистема RSA и ее реализация.	Генерирование публичных ключей и его реализация. Алгоритм криптосистемы RSA. Протокол RSA. Создание криптосистемы RSA.	РЗ
5.	Криптосистема Рабина и ее реализация	Вычисление квадратных корней в классах вычетов. Алгоритм криптосистемы Рабина. Протокол криптосистемы Рабина. Создание криптосистемы Рабина.	РЗ
6.	El Gamel схема кодирования и ее реализация.	Вычисления первообразных корней. Алгоритм вычисления первообразных корней и его реализация. Алгоритм кодирования El Gamel. Протокол El Gamel. Создание криптосистемы El Gamel.	РЗ
7.	Эллиптические кривые и групповая структура на них.	Алгоритм сложения точек на эллиптической кривой и его реализация, графическое представление.	РЗ
8.	Эллиптические кривые над конечными полями и схема кодирования	Построение точек эллиптической кривой над конечным полем. Дискретный логарифм на эллиптической кривой. Создание криптосистемы на основе эллиптической кривой.	РЗ

	рования с помощью эллиптических кривых.		
--	---	--	--

Защита лабораторной работы (ЛР), выполнение курсового проекта (КП), курсовой работы (КР), расчетно-графического задания (РГЗ), написание реферата (Р), эссе (Э), коллоквиум (К), тестирование (Т), типовый расчет (ТР), проверка конспекта (ПК), решение задач (РЗ) и т.д.

2.3.4 Примерная тематика курсовых работ (проектов)

Не предусмотрены.

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1	Проработка учебного (теоретического) материала	«Методические указания по организации самостоятельной работы студентов», утвержденные кафедрой функционального анализа и алгебры, протокол № 1 от 31 августа 2017 г.
2	Выполнение домашних заданий (решение задач)	«Методические указания по организации самостоятельной работы студентов», утвержденные кафедрой функционального анализа и алгебры, протокол № 1 от 31 августа 2017 г.
3	Подготовка к текущему контролю (контрольная работа и др.)	«Методические указания по организации самостоятельной работы студентов», утвержденные кафедрой функционального анализа и алгебры, протокол № 1 от 31 августа 2017 г.
4	Промежуточная аттестация (зачет, экзамен)	«Методические указания по организации самостоятельной работы студентов», утвержденные кафедрой функционального анализа и алгебры, протокол № 1 от 31 августа 2017 г.

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в печатной форме увеличенным шрифтом,
- в форме электронного документа,

Для лиц с нарушениями слуха:

- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

- в печатной форме,
- в форме электронного документа,

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

3. Образовательные технологии.

При изучении данного курса используются традиционные лекции и лабораторные занятия.

Цель лабораторных занятий – научить студента применять полученные на лекциях теоретические знания к решению и исследованию конкретных математических и методических задач. В семестре проводятся контрольные работы для проверки усвоения материала студентами.

Самостоятельная работа студентов является неотъемлемой частью процесса подготовки. Под самостоятельной работой понимается часть учебной планируемой работы, которая выполня-

ется по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

Самостоятельная работа направлена на усвоение системы научных и профессиональных знаний, формирования умений и навыков, приобретение опыта самостоятельной творческой деятельности. СРС помогает формировать культуру мышления студентов, расширять познавательную деятельность.

Виды самостоятельной работы по курсу:

а) по целям: подготовка к лекциям, к практическим занятиям, к контрольной работе, к экзамену, выполнение типового расчета, подготовка проектного семестрового задания в виде презентации.

б) по характеру работы: изучение литературы, конспекта лекций; поиск литературы в библиотеке; конспектирование рекомендуемой для самостоятельного изучения научной литературы; решение задач, подготовка проекта.

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

Интерактивные формы лабораторных занятий:

Интерактивные формы лабораторных занятий			
Се- мест р	Вид занятия	Используемые интерактивные образовательные техно- логии	Количе- ство ча- сов
6	Лабораторные занятия	Коллоквиум на тему: « Простые числа, их распределение. Алгоритмы разложения на простые множители»	4
		Тренинг на тему: «Алгебра и арифметика колец выче- тов»	4
		Метод проектов по теме: «Криптосистемы открытого ключа»	8
Итого:			16

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации.

4.1 Фонд оценочных средств для проведения текущего контроля.

Контрольные работы не предусмотрены.

4.2 Фонд оценочных средств для проведения промежуточной аттестации.

Зачет по курсу не предусмотрен.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в печатной форме увеличенным шрифтом,
- в форме электронного документа.

Для лиц с нарушениями слуха:

- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

- в печатной форме,
- в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

Критерии оценивания по промежуточной аттестации

Зачет выставляется по результатам работы студента в течение семестра. Отметка «зачтено» выставляется студентам, которые регулярно посещали занятия, выполняли домашние работы, написали контрольные работы на положительные оценки. Отметка «незачтено» выставляется студентам, которые пропустили более 60 % занятий и написали контрольные работы на неудовлетворительные оценки.

Оценивание ответа на экзамене, осуществляется по следующим критериям.

Оценка «**отлично**» выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач;

Оценка «**хорошо**» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;

Оценка «**удовлетворительно**» выставляется студенту, показавшему разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет основными разделами учебной программы в некотором объеме, необходимом для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации;

Оценка «**неудовлетворительно**» выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении типовых практических задач.

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля).

5.1 Основная литература:

1. Кострикин, А.И. Введение в алгебру. Часть 3. Основные структуры [Электронный ресурс] : учеб. — Электрон. дан. — Москва : Физматлит, 2001. — 272 с. — Режим доступа: <https://e.lanbook.com/book/59284>.

2. Винберг, Э.Б. Курс алгебры : учебник / Э.Б. Винберг. - Москва : МЦНМО, 2011. - 591 с. - ISBN 978-5-94057-685-3 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=63299>

б) дополнительная литература:

1. Нестеренко В. Основы теории чисел. М. МГУ. 2011.
2. Родосский К. Алгоритм Евклида. М. Наука. 1988.

Для освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья имеются издания в электронном виде в электронно-библиотечных системах «Лань» и «Юрайт».

5.3. Периодические издания:

6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

1. <http://mech.math.msu.su/departament/algebra>
2. <http://www.resolventa.ru/metod/student/determinant.htm>
3. <http://www.exponenta.ru/educat/class/courses/student/an/examples.asp>

7. Методические указания для обучающихся по освоению дисциплины.

Раздел	Тема	Содержание вопросов темы	Вид работы
1	Вопросы 1-3	Простые числа. Основная теорема арифметики. Распределение простых чисел.	Поиск необходимой информации (см. спи-сок литературы). Выполнение домашнего задания.
2	Вопросы 4-7	Разложение на простые множители. Алгоритмы разложения на простые множители. Их сложность.	Поиск необходимой информации (см. спи-сок литературы). Выполнение домашнего задания.
3	Вопрос 8-9	Создание криптосистем открытого ключа.	Поиск необходимой информации (см. спи-сок литературы). Выполнение домашнего задания.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

8.1 Перечень информационных технологий.

Обучающие компьютерные программы по отдельным разделам или темам – не требуются.

8.2 Перечень необходимого программного обеспечения.

Обучающие компьютерные программы по отдельным разделам или темам – не требуются.

8.3 Перечень информационных справочных систем:

1. Электронная библиотечная система eLIBRARY.RU (<http://www.elibrary.ru/>)

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине.

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность
1.	Лекционные занятия	Лекционная аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) и соответствующим программным обеспечением (ПО) 308 Н, 505Н, 507Н;.
2.	Лабораторные занятия	Специальное помещение, оснащенное доской, маркерами и мелом 312Н,314Н, 307Н, 310Н
3.	Групповые (индивидуальные) консультации	Аудитория, (кабинет) 314Н
4.	Текущий контроль, промежуточная аттестация	Аудитория, (кабинет) 308 Н, 505Н, 507Н;312Н,314Н, 307Н, 310Н

5.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета. (309Н, 320Н)
----	------------------------	---